ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT
Journal of Algebra 269 (2003) 373–380
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Stable rationality of certain invariant fields

Esther Beneish [1]

Department of Mathematics, Central Michigan University, Mt. Pleasant, MI 48859, USA

Received 7 September 1997

Communicated by Efim Zelmanov

Abstract

Let F be a field. For a finite group G, let $F(G)$ be the purely transcendental extension of F with transcendency basis $\{x_g\colon g \in G\}$. Let $F(G)^G$ denote the fixed field of $F(G)$ under the action of G. Let w be a primitive $(p-1)$st root of 1, and let I be the ideal $(p, w-a)$ in $Z[w]$ where a is a primitive $(p-1)$st root of $1 \bmod p$. We show that if G be the semi-direct product of a cyclic group of order p by a cyclic group of order prime to p, if I is principal, and if F contains a primitive $|G|$th root of 1, then $F(G)^G$ is stably rational over F. It is not known whether the set of primes p for which I is principal is finite or infinite. We also show that if p is an odd prime and G is a non-abelian group of order p^3, then $F(G)^G$ is stably rational over F provided that F contains a primitive $|G|$th root of 1.

Keywords: Noether settings; Stable rationality; Invariant fields

Introduction

Let F be a field, let G be a finite group G, and let $F(G)$ denote the purely transcendental extension of F with transcendency basis $\{x_g\colon g \in G\}$. Let $F(G)^G$ denote the fixed field of $F(G)$ under the action of G. The question asked by Emmy Noether was: For which F and G is $F(G)^G$ rational over F? This question has been answered in various cases. If G is abelian of exponent n and F contains a primitive nth root of 1, then Fischer [5] showed that $F(G)^G$ is rational over F. In [10], Swan constructed the first example for which $F(G)$ is not rational over F, namely when G is the cyclic group of order 47, and F is the field of rational numbers. Endo, Miyata, Lenstra and Voskresenskii have classified

E-mail address: benei1e@cmich.edu.

[1] Partially supported by NSF grant #DMS-0070665.

0021-8693/$ – see front matter
doi:10.1016/S0021-8693(03)00020-6

the abelian groups G and fields F for which $F(G)^G$ is rational over F [3,8,11]. In [9], Saltman constructs p-groups G, such that $F(G)^G$ is not rational over F, where F is an algebraically closed field of characteristic prime to p. In [7], Hajja has shown that if F is an algebraically closed field of characteristic 0, and if G has an abelian normal subgroup N such that G/N is cyclic of order n and the nth cyclotomic field has class number 0, then $F(G)^G$ is rational over F.

Let p be a prime, and let F be a field. Let G be the semi-direct product of a cyclic group of order p by a cyclic group of order prime to p. Let w be a primitive $(p-1)$st root of 1, and let I be the ideal $(p, w-a)$ in $Z[w]$ where a is a primitive $(p-1)$st root of $1 \bmod p$. We show that if I is principal, and if F contains a primitive pth root of 1, then $F(G)^G$ is stably rational over F, Theorem 1.4. It is not known whether the set of primes p for which I is principal is finite or infinite, however it was proved in [8, Corollary 7.6] that it has Dirichlet density 1. We also show that if p is an odd prime and G is a non-abelian group of order p^3, then $F(G)^G$ is stably rational over F, provided that F contains a primitive $|G|$th root of 1, Theorem 2.3. Some of these groups arose in our study of the stable rationality of the center of the division ring of generic matrices.

1. Let G be a finite group and let M be a ZG-lattice. We will denote by $F(M)$ the quotient field of the group algebra, $F[M]$, of the abelian group M written multiplicatively. Under this notation $F(G)$ is $F(ZG)$.

Definition. Let G be a finite group. A ZG-lattice M is said to be permutation if there exists a Z-basis for M which is permuted by G. A ZG-module is said to be invertible if it is a direct summand of a permutation module. A ZG-module M is said to be stably permutation, if there exist permutation modules P and P' such that $M \oplus P \cong P'$.

Definition. Let L and K be fields on which a finite group G acts. We say that L and K are isomorphic (stably isomorphic) as G-fields if they are isomorphic (stably isomorphic) and the isomorphism respect their G-actions.

Notation. Throughout this article we will use the following notation unless otherwise specified.

F will be a field.
w will be primitive $(p-1)$st root of 1.
a will be primitive $(p-1)$st root of $1 \bmod p$.
I will be ideal $(p, w-a)$ in $Z[w]$.
S will be set of primes p for which I is principal.
For any finite group G and any ZG-lattice M, $\widehat{M}$ will denote the p-adic completion of M, and for any prime q, M_q will denote the localization of M at q.
H will be cyclic group of order p.
C will be cyclic group of order prime to p.
H will be generated by h and C by c.
$G = H \rtimes C$ will be the semi-direct product of H by C.

The following lemma has been proved in the literature in different forms, we include it for the reader's convenience.

Lemma 1.1. *Let G be a finite group, and let V be a finitely generated G-faithful FG-module. Let $F_+(V)$ denote the function field of the symmetric algebra of V. Then for any G-faithful ZG-permutation lattice P, $F_+(V)$ and $F(P)$ are stably isomorphic as G-fields.*

Proof. Let V_1 be the vector space $FP = F \otimes_Z P$. Then $F(P) \cong F_+(V_1)$. Set $L = F_+(V)$ and $L_1 = F_+(V_1)$. Then $F_+(V \oplus V_1) \cong L_+(LV_1) \cong L_{1+}(L_1 V)$. By Speiser's Lemma [12], LV_1^G contains an L-basis for LV_1, say $\{y_1, \dots, y_r\}$, and $L_1 V^G$ contains an L_1-basis for $L_1 V$, say $\{z_1, \dots, z_t\}$. Thus

$$F_+(V \oplus V_1) \cong L(y_1, \dots, y_r) \cong L_1(z_1, \dots, z_t),$$

hence

$$F_+(V)(y_1, \dots, y_r) \cong F(P)(z_1, \dots, z_t)$$

and so $F(P)$ and $F_+(V)$ are stably isomorphic.

Remark. Let $G = H \rtimes C$ be as defined above, and assume that $C = \mathrm{Aut}(H)$ so its order is $p-1$. Since $ZG/H \cong ZC \cong Z[x]/(x^{p-1}-1)$ as ZG-lattices, the decomposition of $\widehat{Z}G/H$ into indecomposables is given by

$$\widehat{Z}G/H \cong \bigoplus_{k=1}^{p-1} Z[x]/\bigl(x-\theta^k\bigr) \cong \bigoplus_{k=1}^{p-1} Z_k,$$

where θ is a primitive $(p-1)$st root of 1 in $\widehat{Z}$ which is congruent to $a \bmod p$, and Z_k is the trivial $\widehat{Z}G$-module of $\widehat{Z}$-rank 1 with trivial H action, and such that $c1 = \theta^k$. We set $X_k = Z_k/pZ_k$, so $X_{p-1} = X$ the trivial $\widehat{Z}G$-module of p elements.

We also have $ZG/C \cong ZH$ where the H-action on ZH is the obvious one and the C-action is given by $ch = h^a$. We will denote by A and A' the ZG-lattices $ZH(h-1)$ and $ZH(h-1)^2$ respectively.

Proposition 1.2. *Let $G = H \rtimes C$ be the semi-direct product of a group H of order p by a cyclic group C equal to* $\mathrm{Aut}(H)$. *The ZG-lattice A is ZC-free, and if $p \in S$, then the ZG-lattice A' is stably permutation as a ZC-lattice.*

Proof. As above we let h generate H and c generate C. A Z-basis for $A = ZH(h-1)$ is $\{h^i - 1\colon i = 1, \dots, p-1\}$, and we have $c(h^i - 1) = h^{ai} - 1$. Thus C permutes the basis elements, and there is a ZC-isomorphism from A to ZC given by $(h-1) \to c$. Now there exists a ZG-exact sequence

$$0 \to A' \to A \to X_1 \to 0$$

with the map $A = ZH(h-1) \to X_1$ given by $h^i(h-1) \to 1$.

Since X_1 is of order p, its localization of at any prime $q \neq p$ is 0, thus $A'_q \cong A_q$. Therefore A' is ZC-cohomologically trivial. By [2, Theorem 8.10, Chapter VI], this implies that A' is ZC-projective.

Let I be the ideal $(p, w-a)$ in $Z[w]$, as defined. Since $Z[w] \cong Z[x]/(\phi(x))$ where $\phi(x)$ is the $(p-1)$st cyclotomic polynomial, there exist a ring map $ZC \to Z[w]$ given by $1_{ZC} \to 1_{Z[w]}$. Thus $Z[w]$ is a ZC-module where c acts by multiplication by w. Furthermore, the map of ZC-modules $Z[w] \to X_1$ has kernel I. We have the following commutative diagram of ZC-modules:

$$\begin{tikzcd}
 & & 0 & 0 & \\
0 \arrow[r] & A' \arrow[r] & A \arrow[r] \arrow[u] & X_1 \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & A' \arrow[r] \arrow[u] & M \arrow[r] \arrow[u] & Z[w] \arrow[r] \arrow[u] & 0 \\
 & & I \arrow[r] \arrow[u] & I \arrow[u] & \\
 & & 0 \arrow[r] \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

where M is the pullback of the maps $A \to X_1$ and $Z[w] \to X_1$.

For a ZC-lattice E, let $E^* = \mathrm{Hom}_Z(E, Z)$ be its dual. Since A' is ZC-projective, so is A'^*, therefore $M^* \cong A'^* \oplus Z[w]^*$, and we have

$$M \cong A' \oplus Z[w] \cong A \oplus I \cong ZC \oplus I.$$

If $p \in S$, I is principal, and therefore it is isomorphic to $Z[w]$ as a ZC-module. By [4, Theorem 4.2], this implies that A' is stably permutation as a ZC-lattice.

Theorem 1.3. *Let p be a prime in S. Let $G = H \rtimes C'$ be the semi-direct product of a group H of order p by a cyclic group C' contained in* Aut(H). *Then $F(G)^G$ is stably rational over F provided that F contains a primitive $|G|$th root of* 1.

Proof. Let $C = \mathrm{Aut}(H)$, so C is of order $p-1$. Consider the ZC-exact sequence of Proposition 1.2, namely

$$0 \to A' \to A \to X_1 \to 0.$$

Restricting to C, and using the fact that $A \cong ZC$ by Proposition 1.2, we get the ZC-sequence

$$0 \to A' \to ZC \to X_1 \to 0.$$

Let F^* be the multiplicative group of F, and let $Y = \mathrm{Hom}(X_1, F^*)$ be the character group of X_1. By Galois theory there is a linear action of $Y \rtimes C$ on $F(ZC)$ such that

$$F(ZC)^{Y \rtimes C} \cong F\big(A'\big)^C$$

and for any subgroup K of C

$$F(ZC)^{Y \rtimes K} \cong F\big(A'\big)^K.$$

In particular,

$$F(ZC)^{Y \rtimes C'} \cong F\big(A'\big)^{C'}.$$

Now as a group $G \cong Y \rtimes C'$. Let V the FG-module with F-basis $\{x_1, \dots, x_{p-1}\}$ where G acts on x_i as on c^i for $i = 1, \dots, p-1$. Then V is G-faithful and $F(ZC) \cong F_+(V)$. By Lemma 1.1, $F(G)$ is G-stably isomorphic to $F(ZC)$, hence $F(G)^G$ is stably isomorphic to $F(A')^{C'}$. Since A' is ZC'-stably permutation by Proposition 1.2, $F(A')$ is stably isomorphic to $F(ZC)$ as a C'-field by [1, Lemma 2.1]. The result now follows by [5] since C' is abelian.

Theorem 1.4. *Let G be the semi-direct product of a group H of order p, by a group C of order prime to p. Let w be a primitive $(p-1)$st root of 1, and let I be the ideal $(p, w-a)$ in $Z[w]$, where a is a primitive $(p-1)$st root of $1 \bmod p$. If I is principal then $F(G)^G$ is stably rational over F provided that F contains a primitive $|G|$th root of 1.*

Proof. Let $G = H \rtimes C$. Let $C' = \mathrm{Ker}(C \to \mathrm{Aut}(H))$, then C' is normal in G. By Lemma 1.1, $F(G)$ is stably isomorphic as a G-field to $F_+(V)$ for any faithful FG-lattice V. Let

$$V = F \otimes_Z ZG/C \oplus W,$$

where W is a one-dimensional faithful representation of C, with trivial H-action. Then

$$F_+(V)^G = \big(F_+(V)^{C'}\big)^{G/C'}.$$

It is immediate that $F_+(V)^{C'}$ is stably isomorphic to $F(ZG/C)$ as a G/C'-field. Thus $F(G)^G$ is stably isomorphic to $F(ZG/C)^{G/C'}$. But $G/C' \cong H \rtimes K$, where $K = C/C'$ is a subgroup of $\mathrm{Aut}(H)$. The result then follows by Theorem 1.3.

2. Let p be an odd prime. In this section we show that if G is a non-abelian group of order p^3, then $F(G)^G$ is stably rational over F. By [6, Theorem 5.1, Chapter 5] there exists, up to isomorphism, two groups satisfying these conditions. They are the semi-direct products of a group of order p^2 by a group of order p. The group of order p^2 is cyclic in one case and p-elementary in the other.

Proposition 2.1. *Let H be a cyclic group of order p, with generator h. There exists an exact sequence*

$$0 \to ZH(h-1)^2 \oplus Z \to ZH \to D \to 0,$$

where D is a ZH-module of order p^2 and exponent p.

Proof. Consider the ZH-exact sequence

$$0 \to ZH(h-1)^2 \oplus Z \to ZH \to D \to 0,$$

where the map $ZH(h-1)^2 \oplus Z \to ZH$ is inclusion on $ZH(h-1)^2$ and sends 1_Z to the trace, N, of H. The ZH-module $D \cong ZH/(ZH(h-1)^2, N)$. The following part of this proof was suggested by the referee, and it is much simpler than my original proof. Using $y = h-1$ as a new variable, we have

$$D \cong Z[y]/\bigl(y^2, N\bigr).$$

It is easily checked that

$$p = \sum_{i=1}^{p-1} i(y+1)^i y + N,$$

and that

$$N = p + py(p-1)/2 \bmod \bigl(y^2\bigr).$$

Therefore $py = 0$ and $N = p$ in D. Thus $D \cong Z[y]/(y^2, py, p) \cong k[y]/(y^2)$ where $k = Z/pZ$. Thus D has exponent p. Clearly the H-action on D is not trivial.

Remark. Let $D' = \mathrm{Hom}(D, F^*)$. The group $G = D' \rtimes H$ is of exponent p since for any $d \in D'$, $(dh^i)^p$ is equal to the norm of the subgroup of D' generated by d, and thus is equal to 1.

Notation. For all n in Z, for any finite group G and ZG-module M, $H^n(G, M)$ will denote the nth Tate cohomology group of G with coefficients in M.

Proposition 2.2. *Let G be a group of order p^3 having a cyclic subgroup K' of index p. Let $H = G/K'$, and let $K = \mathrm{Hom}(K', F^*)$. Then there exists a ZH-exact sequence*

$$0 \to ZH \to ZH \to K \to 0.$$

Proof. By [6, Theorem 5.1, Chapter 5] there exists, up to isomorphism, a unique group of order p^3 having a cyclic subgroup of index p. It is the semi-direct product of this cyclic group of order p^2 by a group of order p. Therefore $K \cong K'$ as ZH-modules, and $G \cong K' \rtimes H$. Let N be the trace of H. There is a ZH-exact sequence

$$0 \to ZH \to ZH \to T \to 0, \tag{1}$$

where the map $ZH \to ZH(h-1) \oplus Z$ sends 1 to $(h-1) + N$. It is easily checked that the map is injective.[2]

We have $T \cong ZH/(h - 1 + N)$. Again using the new variable $y = h - 1$, it is trivial to check that

$$T \cong Z[y]/\bigl(y^2, p, p + y\bigr) \cong Z/p^2 Z$$

and clearly the H-action on T is not trivial. Setting $T = K$ the result is proved.

Theorem 2.3. *Let p be an odd prime. Let G be an abelian group of order p^3, and let F be a field containing a primitive p^2th root of* 1. *Then $F(G)^G$ is stably rational over F.*

Proof. Let H, K and D be as in Propositions 2.1 and 2.2. Let $K' = \mathrm{Hom}(K, F^*)$ and $D' = \mathrm{Hom}(D, F^*)$ be the character groups of S and D, respectively. By [6, Theorem 5.1, Chapter 5] G is isomorphic to either $K' \rtimes H$ or to $D' \rtimes H$.

Case 1. $G \cong K' \rtimes H$.

By Proposition 2.2, we have a ZH-exact sequence

$$0 \to ZH \to ZH \to K \to 0.$$

By Galois theory $F(ZH)^G \cong F(ZH)^H$, which is rational over F, by [5]. Therefore $F(ZH)^G$ is stably rational over F. By Lemma 1.1, $F(G)^G$ is stably isomorphic to $F(ZH)^G$ which proves the result.

Case 2. $G \cong D' \rtimes H$.

By Proposition 2.1 there exists a ZH-exact sequence

$$0 \to ZH(h-1)^2 \oplus Z \to ZH \to D \to 0.$$

By Galois theory $F(ZH(h-1)^2 \oplus Z)^H \cong F(ZH)^G$. Now $ZH(h-1)$ and $ZH(h-1)^2$ are isomorphic as ZH-modules and the isomorphism is given by

$$h^i(h-1) \to h^i(h-1)^2.$$

[2] The following part of this proof was suggested by the referee and it is much simpler than my original proof.

Thus $F(ZH(h-1)^2 \oplus Z)^H \cong F(ZH(h-1) \oplus Z)^H$. We have a ZH-exact sequence

$$0 \to ZH(h-1) \to ZH \to Z \to 0,$$

and by [1, Lemma 1.2] $F(ZH(h-1) \oplus Z)$ and $F(ZH)$ are isomorphic as H-fields. Therefore $F(ZH)^G$ and $F(ZH)^H$ are stably isomorphic and the argument now is the same as in Case 1.

Acknowledgment

The author wishes to thank the referee for a very in-depth report, and for suggesting simpler proofs of some of the results.

References

[1] E. Beneish, Induction theorems on the center of the ring of generic matrices, Trans. Amer. Math. Soc. 350 (9) (1998) 3571–3585.
[2] K. Brown, Cohomology of Groups, Springer-Verlag, New York, 1982.
[3] S. Endo, T. Miyata, Invariants of finite abelian groups, J. Math. Soc. Japan 25 (1973) 7–26.
[4] S. Endo, T. Miyata, Quasi-permutation modules over finite groups II, J. Math. Soc. Japan 26 (1974) 698–713.
[5] E. Fischer, Die Isomorphie der Invariantenkorper der endlichen Abel'schen Gruppen linearen Transformationen, Nachr. Konigl. Ges. Wiss. Gottingen (1915) 77–80.
[6] D. Gorenstein, Finite Groups, Harper & Row, 1968.
[7] M. Hajja, Rational invariants of meta-abelian groups of linear automorphisms, J. Algebra 80 (1983) 295–305.
[8] H.W. Lenstra, Rational functions invariant under a finite abelian group, Invent. Math. 25 (1974) 299–325.
[9] D. Saltman, Noether's problem over an algebraically closed field, Invent. Math. 77 (1984) 71–84.
[10] R. Swan, Invariant rational functions and a problem of Steenrod, Invent. Math. 7 (1969) 148–158.
[11] V.E. Voskresensskii, Rationality of certain algebraic tori , Izv. Akad. Nauk SSSR Ser. Mat. 35 (1971) 1037–1046, Russian; English translation: Math. USSR-Izv. 5 (1971) 1049–1056.
[12] D.J. Winter, The Structure of Fields, Springer-Verlag, 1974.

Further reading

[1] Curtis, Reiner, Methods of Representation Theory, Vol. 1, Wiley, New York, 1981.
[2] S. Endo, T. Miyata, On the classification of the function fields of algebraic tori, Nagoya Math. J. 56 (1974) 85–104.